ABSTRACT

A method, system, and apparatus for performing computations.

In a method, arguments X and K are loaded into session memory, and X mod P and X mod Q are computed to give, respectively, X_P and X_Q. X_P and X_Q are exponentiated to compute, respectively, C_P and C_Q. C_P and C_Q are merged to compute C, which is then retrieved from the session memory.

A system includes a computing device and at least one computational apparatus, wherein the computing device is configured to use the computational apparatus to perform accelerated computations.

An apparatus includes a chaining controller and a plurality of computational devices. A first chaining subset of the plurality of computational devices includes at least two of the plurality of computational devices, and the chaining controller is configured to instruct the first chaining subset to operate as a first computational chain.